WAP 7.13.07 Please replace the paragraph beginning at page 17, line 12 with the following amended paragraph:

Figure 8 is a diagram illustrating a first example of a second embodiment of the mobile application security system 50 for preventing hostile hosts from transmitting code to other hosts in accordance with the invention. In particular, the mobile application 40 is created by Host1 and then later dispatched to another host to continue the execution of the mobile application 40. In this example, Host1 is untrusted in that the server 52 does not know whether or not to trust the host when interacting with the mobile application 40. Therefore, the mobile application 40 dispatched from Host1 is sent to the server 52 in accordance with the invention and the server 52 may perform several security measures. For example, it may strip any code from the mobile application 40 and store an (empty) copy of the mobile application code in the database 62. The server 52 may alternatively check the code to ensure that it is safe and forward only safe code to the next host. The server 52 may then forward the mobile application 40 onto the next host, Host2 in this example. The mobile application 40 may then be received by and executed by Host2. When the mobile application 40 requires code for execution, the tested version of the code may be supplied to Host2 by the server 52 thus ensuring that the untrusted host cannot spread a virus, for example, using the mobile application 40. Now, the dispatch of a mobile application from a trusted host to another host will be described.

WAP 7.13.07 Please replace the paragraph beginning at page 18, line 8 with the following amended paragraph:

Figure 9 is a diagram illustrating a second example of a second embodiment of the mobile application security system 50 for preventing hostile hosts from transmitting code to other hosts in accordance with the invention. In particular, the mobile application 40 is created by Host1 and then later dispatched to another host to continue the execution of the mobile application 40. In this example, Host1 is trusted in that the server 52 knows that the particular host is trusted and therefore does not need to strip the code from the mobile application 40 and test it as described above. Therefore, the mobile application 40 dispatched from Host1 is sent to the server 52 in accordance with the invention and the server 52 may store a copy of the mobile

application code in the database 62. The server 52 may then forward the mobile application 40 onto the next host, Host2 in this example. The mobile application 40 may then be received by and executed by Host2. When the mobile application 40 requires the code for execution, the known safe version of the code may be supplied to Host2 by the server 52 or, since the originating host is trusted, the code may be provided by the originating host. Now, the subsequent dispatch of a mobile application from an untrusted host will be described.

WP 7.13.07 Please replace the paragraph beginning at page 18, line 19 with the following amended paragraph:

Figure 10 is a diagram illustrating a third example of a second embodiment of the mobile application security system 50 for preventing hostile hosts from transmitting code to other hosts in accordance with the invention. In particular, the mobile application 40 is received from another host by an untrusted host (Host n) and then later dispatched to another host to continue the execution of the mobile application 40. In this example, Host n is untrusted in that the server 52 does not know whether the particular host may perform nefarious acts on the mobile application or using the mobile application. Therefore, the mobile application 40 dispatched from Host n is sent to the server 52 in accordance with the invention and the server 52 may perform several security measures. For example, the server 52 may receive the code of the mobile application 40 and compare the current code to a previously stored version of the code to ensure that the newly received code is the same as the previous code. The server 52 may then forward the mobile application 40 onto the next host, Host n+1 in this example. The mobile application 40 may then be received by and executed by Host n+1. When the mobile application 40 requires code for execution, the known safe version of the code may be supplied to Host n+1 by the server 52 or, if the originating host is trusted, the code may be provided by the originating host. Now, the subsequent dispatch of a mobile application from a trusted host will be described.

WP 7.13.07 Please replace the paragraph beginning at page 19, line 14 with the following amended paragraph:

Figure 11 is a diagram illustrating a fourth example of a second embodiment of the